

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-6, 8-16, and 18-22 are currently pending, Claims 1-6, 8-16, and 18-22 having been amended. The changes and additions to the claims do not add new matter and are supported by the originally filed specification, for example, on Fig. 14; and page 48, lines 4-14.

In the outstanding Office Action, Claims 2-6, 10, 12-16, 18, and 20 were objected to for informalities; the specification was objected for failing to provide proper antecedent basis for the claimed subject matter; Claims 1-6, 8-16, and 18-22 were rejected under 35 U.S.C. §112, first paragraph as failing comply with the written description requirement; Claims 1-6, 8-16, and 18-22 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite; Claims 1-6, 8-16, and 18-20 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter; Claims 1-5, 9-15, 19 and 22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier ("Applied Cryptography," Second Edition) in view of Bo Lin et al. (GB 2345229A, hereafter "Lin"); Claims 6 and 16 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Lin and Kocher et al. (U.S. Pub. No. 2001/0053220A1, hereafter "Kocher"); and Claims 8 and 18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Lin and Kaminaga et al. (U.S. Pub. No. 2002/0124179A1, hereafter "Kaminaga").

Applicants thank the examiner and his supervisor for the courtesy of an interview with Applicants' representative, Mr. Sameer Gokhale, on November 12, 2009. During the interview, Mr. Gokhale explained the features of the Applicants' invention to the examiner. Mr. Gokhale further explained the differences between the claims and the applied art. Clarifying amendments were discussed to overcome the rejections under 35 U.S.C. §112 and

35 U.S.C. §103(a). No agreement was reached. The claims and arguments presented herewith are similar to those discussed during the interview.

With respect to the objection to Claims 2-6, 10, 12-16, 18, and 20 for informalities, Applicants submit that the present amendment to Claims 2-6, 8, 10, 12-16, 18, and 20 overcomes this ground of objection.

With respect to the objection to the specification, the rejection of Claims 1-6, 8-16, and 18-22 under 35 U.S.C. §112, first paragraph, and the rejection of Claims 1, 9, 11, 19, and 21-22 under 35 U.S.C. §112, second paragraph, the Office Action takes the position that the feature of “said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups so that performance of at least one encryption processing unit from one of the groups is performed at a time between performance of encryption processing units from another one of the groups,” is not found in the specification. Amended Claim 1 now recites “said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group.”

Page 32, line 2 to page 33, line 9 of the Applicants’ specification states the following:

These DES encryption processes are performed with their sequences being replaced. However, for example, in the X group, X2 is performed after X1, and thereafter, X3, X4, X5, and X6 must be performed in this order. Therefore, the change of this processing sequence of X1 to X6 is not performed. Also, in the Y group, Y2 is performed after Y1, and thereafter, Y3, Y4, Y5, and Y6 must be performed in this order. Therefore, the change of this processing sequence of Y1 to Y6 is not performed.

In the encryption processing apparatus of the present invention, a mixed encryption processing sequence is set by dividing the original encryption processing sequence into a plurality of groups composed of one or more encryption processing units, and by performing a mixing of the processing sequences of the encryption processing units under the condition in which the processing sequence of the encryption processing units within each set group is fixed.

The number of combinations of the cases in which, under the above-described conditions, the processing sequences of the processing units X1 to X6 and Y1 to Y6 + n of the single-DESs which form the X group and the Y group are mixed is calculated as described below.

First, as shown in Fig. 8A, there are a plurality of processing modes in which a Y group is inserted before and after X1 to X6 of the X group and in between them. For example, in a mode of a case in which a Y group, which is made a cluster, is inserted at the positions a1 to a7 of the X group shown in Fig. 8A, 7C_1 kinds, that is, 7 kinds. Furthermore, in a mode of a case in which a Y group is divided into two parts and these are inserted at the positions a1 to a7 of the X group shown in Fig. 8A, 7C_2 kinds, that is, 21 kinds. Hereafter, the Y group can be divided up to 6 + n, and in that case, there are combinations of ${}^7C_{6+n}$.

Thus, the specification clearly describes an example of “said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit [X1] from the first group [X] at a time between executing performance of encryption processing units [Y1...Y2] from the second group [Y].”

Therefore, Applicants respectfully submit that the specification does clearly provide support for the feature of “said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group,” as defined by Claim 1.

Therefore, Applicants respectfully request that the objection to the specification, and the rejections under 35 U.S.C. §112, first paragraph and second paragraph be withdrawn.

With respect to the rejection of Claims 1, 9, 11, 19, and 21-22 under 35 U.S.C. §112, second paragraph, the Office Action takes the position that the phrase “where the input data to be encrypted for one of the groups is different” is unclear. Applicants submit that the present amendment to Claim 1 (and similarly Claims 9, 11, 19, and 21-22), reciting “where the input data to be encrypted for a first group of the groups is different relative to the input data to be encrypted for a second group of the groups, and the input data to be encrypted for the first group is generated independently relative to the input data to be encrypted for the second group,” overcomes this ground of rejection.

With respect to the rejection of Claims 8 and 18 under 35 U.S.C. §112 second paragraph, Applicants respectfully submit that the present amendment to Claims 8 (and similarly Claim 18), reciting “said control section is configured to store the processing results in said memory to identify which encryption processing unit the processing results are obtained from,” overcomes this ground of rejection.

With respect to the rejection of Claim 12, under 35 U.S.C. §112 second paragraph, Applicants respectfully submit that the present amendment to Claim 12, reciting “said dummy encryption processing unit,” overcomes this ground of rejection.

With respect to the rejection of Claims 1-6 and 8-10 under 35 U.S.C. §101, Applicants respectfully submit that the present amendment to independent Claims 1 and 9, which recite that the encryption processing apparatus comprises at least a “processor” overcomes this ground of rejection.

With respect to the rejection of Claims 11-16 and 18-20 under 35 U.S.C. §101, Applicants respectfully submit that the present amendment to independent Claims 11 and 19,

clarifying that the claimed method is implemented on an “encryption processing apparatus,” and is thus tied to a particular machine or apparatus, overcomes this ground of rejection.

With respect to the rejection of Claim 1 under 35 U.S.C. §103(a), Applicants respectfully traverse this ground of rejection and further submit that the clarifying amendments to Claim 1 overcome this ground of rejection. Amended Claim 1 recites, *inter alia*,

a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for a first group of the groups is different relative to the input data to be encrypted for a second group of the groups, and the input data to be encrypted for the first group is generated independently relative to the input data to be encrypted for the second group, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group and under a condition in which a processing sequence of the encryption processing units within each of the plurality of groups is fixed.

As previously presented, in a non-limiting example, Applicants' Fig. 5 shows a conventional authentication procedure between a reader/writer and an IC card. In S101, a random number R_r is input into a triple-DES encryption process, and encrypted data A1 is generated. In S102, the IC card receives the encrypted data A1, and decrypts it to obtain decrypted data A1_1. The decrypted data A1_1 is input into another triple-DES process to obtain encrypted data B1. Also, the IC card inputs a random number R_c into a triple-DES process to generate encrypted data B2. Thus, in the IC card, one group may be the process which inputs A1 and outputs encrypted data A1_1, while another group is the process which

inputs random number Rc and outputs B2. Additionally, in this non-limiting example, an “encryption unit” may be a single-DES round within the triple-DES process. Thus, it is clear that there is “each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to the input data to be encrypted for another one of the groups,” because Rc and A1 are created completely independently of each other. Applicants’ Figs. 6A and 6B show that in a conventional case, these groups would be performed in sequence, such that the process for inputting Rc into a triple-DES process to produce B2 is not performed until the process of producing A1_1 and B1 is performed. Thus, Fig. 6A is an example of an original encryption processing sequence. However, Applicants’ Fig. 8 shows a non-limiting example of the present invention where the sequence is mixed. Fig. 8 shows that the single DESs which are encryption processing units used in the generation of B2, are inserted between the single DESs which are used to generate A1_1 and B1. Thus, these two separate and independent encryption groups, which have separate and independent inputs (A1 and Rc) are mixed together.

Applicants respectfully submit that the combination of Schneier and Lin fails to disclose or suggest all of the features Claim 1.

Schneier is directed to a description of the Data Encryption Standard (DES) and combining block ciphers. In chapter 12, Schneier describes conventional DES, which includes 16 rounds in which a function which uses a key is applied on a plaintext block 16 times (see pages 270-278 of Schneier). In chapter 15, Schneier then describes ways to combine block algorithms to get new algorithms to increase security without designing a new algorithm. In Chapter 15, Schneier describes Double Encryption and Triple Encryption. In Triple Encryption, a ciphertext block is operated on three times with multiple keys (see pages 357-361 of Schneier). Schneier describes different permutations of Triple Encryption based

on the types of keys used (see page 360, describing Triple Encryption with Three Keys and Triple Encryption with Minimum Key). Schneier also describes different modes of Triple Encryption involving Cipher Block Chaining (CBC), such as “Inner-CBC” and “Outer-CBC” (see page 360).

With regard to the feature of “dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units,” the Office Action states that “DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times.” The Office Action also cites to the above-mentioned triple encryption described in Chapter 15 of Schneier. (See Office Action, at pages 3 and page 5). Therefore, it appears that the Office Action believes that a DES block having 16 rounds, the triple encryption in CBC mode, or the triple-DES encryption can correspond to “a plurality of groups composed of one or more encryption processing units.”

However, amended Claim 1 recites that “*each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for a first group of the groups is different relative to the input data to be encrypted for a second group of the groups, and the input data to be encrypted for the first group is generated independently relative to the input data to be encrypted for the second group.*” Therefore, each group in Claim 1 is a separate and independent encryption process with separately and independently generated input data.

However, as presented in the Applicants’ previous response, in the Triple Encryption described by Schneier, including both Inner-CBC and Outer-CBC modes, *encryption is being applied to a single plaintext file* (see page 360, for example, where Schneier describes encrypting “the entire file” for each of the Inner-CBC and Outer-CBC modes). Additionally, a single DES with 16 rounds still has just one independently generated input (the initial

input), because any subsequent input into any of the later rounds is derived from an input from the previous round. Thus, any one of these processes being described in Schneier constitutes only a single group as defined by Claim 1 because each of the processes described in Schneier is still just directed to a single independently generated input being put through an overall encryption process to produce a single encrypted output.

Applicants note that the Office Action has not addressed the Applicants' previous arguments directly, and has cited to Schneier without actually articulating how Schneier discloses "each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to the input data to be encrypted for another one of the groups," as was recited in previously presented Claim 1.

Therefore, Applicants submit that the Office Action has not clearly shown that Schneier discloses "each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to the input data to be encrypted for another one of the groups," as recited in previous Claim 1. Accordingly, Applicants submit that the Schneier fails to disclose or suggest "each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for a first group of the groups is different relative to the input data to be encrypted for a second group of the groups, and the input data to be encrypted for the first group is generated independently relative to the input data to be encrypted for the second group," as now clarified in amended Claim 1.

Applicants note that the Office Action further acknowledges that Schneier fails to disclose or suggest "by inserting at least one encryption processing unit from one of the

groups between encryption processing units from another one of the groups,” as previously recited in Claim 1. (See Office Action, at page 10).

Accordingly, Applicants submit that Schneier also fails to disclose or suggest “said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group.”

The Office Action relies on Lin to remedy this deficiency of Schneier.

Lin describes inserting dummy S-block lookups into a real DES process (see page 11, lines 10-13). However, *an dummy S-block lookup in Lin does not have its own input data to be encrypted*, and therefore they do not form a first or second “group” as defined in Claim 1 in which “each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for a first group of the groups is different relative to the input data to be encrypted for a second group of the groups, and the input data to be encrypted for the first group is generated independently relative to the input data to be encrypted for the second group.”

Additionally, there is not a group of dummy S-block lookups in Lin which has a single independent input and further includes “a plurality of encryption processing units,” as defined by amended Claim 1. In other words, if the real DES process of Lin corresponds to the “the first group” in Claim 1, then the collection of dummy S-block lookups is not “a second group” because it does not separately encrypt a single input data which is generated independently.

Therefore, Applicants submit that Lin does not disclose or suggest “said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the

first group at a time between executing performance of encryption processing units from the second group,” according to a “first group” and a “second group” which are defined in amended Claim 1.

Thus, Applicants submit that Lin fails to remedy the deficiencies of Schneier with regard to Claim 1.

Therefore, Applicants submit that amended Claim 1 (and all associated dependent claims) patentably distinguishes over Schneier and Lin, either alone or in proper combination.

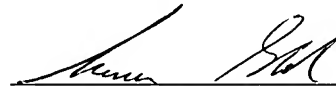
Kocher and Kaminaga have been considered but fail to remedy the deficiencies of Schneier and Lin with regard to Claim 1. Thus, Applicants respectfully submit that amended Claim 1 (and all associated dependent claims) patentably distinguishes over Schneier, Lin, Kocher, and Kaminaga, either alone or in proper combination.

Independent Claims 9, 11, 19, 21, and 22 recite features similar to those of amended Claim 1. Thus, Applicants respectfully submit that Claims 9, 11, 19, 21, and 22 (and all associated dependent claims) patentably distinguish over Schneier, Lin, Kocher, and Kaminaga, either alone or in proper combination.

Consequently, in light of the above discussion and in view of the present amendment, the outstanding grounds for rejection are believed to have been overcome. The present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)

Sameer Gokhale
Registration No. 62,618